HOPLOS
VOL. 06 N° 10/2022

Bernardo Wahl Gonçalves de Araújo Jorge

Professor de Pós-Graduação (FESPSP) e de Bacharelado (FMU) em Relações Internacionais (RI). Mestre em Relações Internacionais pelo Programa San Tiago Dantas (UNESP, UNICAMP e PUC-SP) e Bacharel em Relações Internacionais pela Universidade de São Paulo (USP).

A DIMENSÃO CIBERNÉTICA DA GUERRA ENTRE A RÚSSIA E A UCRÂNIA EM 2022: UMA AVALIAÇÃO INICIAL PASSADOS 100 DIAS DO CONFLITO

THE CYBER DIMENSION OF THE RUSSIA/UKRAINE WAR IN 2022: AN INITIAL ASSESSMENT AFTER 100 DAYS OF THE CONFLICT

RESUMO: O presente artigo busca examinar com mais detalhes a dimensão cibernética dos primeiros cem dias da guerra entre a Rússia e a Ucrânia em 2022. Foram identificadas basicamente duas hipóteses sobre isso: a primeira aponta que a guerra cibernética não se desenvolveu como era esperado; a segunda indica que houve uma ampla campanha de guerra cibernética. A partir de ambas as hipóteses, pode-se chegar a uma terceira, de síntese: o que vem ocorrendo é uma forma de guerra cibernética mais "branda", ou de baixa intensidade. Para auxiliar na compreensão do objeto estudado, esta análise também contará com uma seção dedicada ao entendimento dos significados de guerra cibernética.
Palavras-chave: Rússia x Ucrânia; Guerra cibernética; Sabotagem; Espionagem; Subversão.

ABSTRACT: This article seeks to examine in more detail the cybernetic dimension of the first hundred days of the war between Russia and Ukraine in 2022. Basically, two hypotheses were identified: the first one points out that the cybernetic war did not develop as expected; the second indicates that there was a widespread cyberwarfare campaign. Based on both hypotheses, we can arrive at a third, a synthesis: what has been happening is a more "mild" or low-intensity form of cyber warfare. To assist in understanding the object studied, this analysis will also have a section dedicated to comprehend the meanings of cyber warfare.
Keywords: Russia vs Ukraine; Cyber warfare; Sabotage; Espionage; Subversion.

1 Introdução

Difundida na imprensa e por analistas ocidentais, existe uma visão (entre outras visões) que aponta o seguinte: a "operação militar especial", ou guerra convencional, iniciada por Moscou na Ucrânia em 24 de fevereiro de 2022 não se desenrolou como era inicialmente previsto entre os especialistas[1], os quais acreditavam que uma grande potência nuclear como a Rússia poderia ter obtido uma vitória breve e decisiva sem maiores dificuldades, embora esse tipo de conjectura seja dificultada por não se entender claramente os reais objetivos de Moscou e pelo fato de que, conforme ensinou Sun Tzu, "toda guerra é baseada na dissimulação" (TZU, 2006, p. 25). Em 03 de junho de 2022, momento da finalização deste artigo, completaram-se cem dias de confronto armado, que permanece indefinido, manifestando-se atualmente sob a forma de uma guerra prolongada de atrito (ou desgaste), o que significa que ambos os lados (Rússia e Ucrânia – esta última com apoio do mundo ocidental) buscam reduzir a capacidade física do adversário para lutar.

E na dimensão cibernética, o que foi descrito anteriormente também se aplica, isto é, não ocorreu conforme o esperado? A expectativa de especialistas ocidentais em ciber segurança (MARKS; SCHAFFER, 2022; MENN; TIMBERG, 2022) era que Moscou, com o uso da guerra cibernética, pudesse ter neutralizado não apenas as defesas militares ucranianas, mas eventualmente toda a sociedade, para assim facilitar a imposição de sua vontade. Porém, a Ucrânia não foi "apagada do mapa" (no sentido figurado, obviamente) nem antes, nem durante e nem após a invasão militar russa (embora não se tenha certeza de que o Kremlin buscasse realmente "desligar" o país invadido). O que explica isso?

Através da revisão de notícias e artigos, foram identificadas basicamente duas hipóteses sobre a dimensão cibernética nos primeiros cem dias do conflito armado Rússia x Ucrânia em 2022: a primeira aponta que a ciber guerra não se desenvolveu como era esperado (ABBANY, 2022; HALPERN, 2022; RM STAFF, 2022; ROHOZINSKI, 2022; WOLFF, 2022); a segunda, oposta à anterior, indica ser um "mito" a ausência de guerra cibernética (CATTLER; BLACK, 2022; RID, 2022). A partir das hipóteses prévias, a corrente investigação chega a uma terceira hipótese de trabalho, que sintetiza as anteriores e orienta a pesquisa apresentada neste

[1]Ver, por exemplo (referências completas disponíveis na bibliografia deste artigo): (i) DONATO, J. M. "Putin's Bad Math: the Root of Russian Miscalculation in Ukraine"; (ii) FREEDMAN, L. "Putin's war is in disarray"; (iii) JOHNSON, R. "Dysfunctional Warfare: The Russian Invasion of Ukraine 2022"; (iv) JOHNSON, D. "Putin's catastrophic war has exposed Russia as a third-rate power"; (v) HEDLUND, S. "The collapse of the Russian military machine"; (vi) MASUHR, N.; ZOOG, B. "The War in Ukraine: First Lessons"; (vii) SHULTZ, R.; BRIMELOW, B. "Russia's Potemkin Army", entre outros.

empreendimento intelectual: o que ocorreu, e vem ocorrendo, entre a Rússia e a Ucrânia é uma forma de guerra cibernética mais "branda" (ou de baixa intensidade).

Da mesma forma que, conforme apontado por Carl von Clausewitz (1996), existe a chamada "névoa da guerra" (isto é, o problema em saber o que realmente está ocorrendo no enfrentamento bélico), igualmente há uma "névoa da guerra cibernética", o que dificulta saber tudo o que está acontecendo no ciberespaço. Somado a isso, também deve ser levado em conta o problema da atribuição no espaço cibernético (quer dizer, saber exatamente quem está fazendo o quê e porquê). Entretanto, isso não impede a elaboração de conjecturas e hipóteses (preferencialmente baseadas em fatos observáveis e podendo ser confirmadas ou negadas por novas informações que venham a surgir) para adequado entendimento do fenômeno.

Este artigo busca compreender melhor a questão levantada anteriormente, estando o presente texto organizado em quatro partes: (1) Introdução; (2) Guerra cibernética: em busca de uma definição; (3) A guerra cibernética entre a Rússia e a Ucrânia em 2022 (3.1 Primeira hipótese: não aconteceu como se esperava, 3.2 Segunda hipótese: o mito da guerra cibernética ausente e 3.3 Terceira hipótese: síntese das anteriores) e; (4) Considerações finais.

2 Guerra cibernética: em busca de uma definição[2]

Uma revisão da literatura internacional apontou que não há uma definição amplamente aceita de guerra cibernética (ROBINSON; JONES; JANICKE, 2015). Apesar da ideia do confronto no ciberespaço ter se revelado na consciência pública desde os anos 1980, não há uma visão largamente compartilhada sobre o que isso quer dizer. Existem inúmeras noções distintas e muitas vezes opostas, que vão desde a inexistência da guerra cibernética até esta como uma ameaça existencial. Durante quase três décadas, os especialistas têm oferecido definições variadas do fenômeno, e a falta de clareza contínua testemunha que os esforços para estabelecer uma definição singular não foram bem sucedidos. Levando isso em consideração, pode-se dizer que é improvável que apareça uma definição acadêmica amplamente aceita e consensual de guerra cibernética, pelo menos no horizonte previsível (ASHRAF, 2021).

Expondo a variedade de significados, Hughes e Colarik (2017) examinaram 159 publicações e identificaram 56 definições explícitas e 103 implícitas de guerra cibernética

[2]Uma reflexão acerca do significado de guerra cibernética foi desenvolvida pelo autor na *live streaming* (transmissão ao vivo) "O que é guerra cibernética?", disseminada pelo *in_CYBER* (boletim com notícias de segurança cibernética elaborado pelo jornalista Paulo Brito, um dos responsáveis pelo portal *CISO Advisor*, especializado em informações sobre defesa, segurança e inteligência cibernéticas) em 07 de janeiro de 2022. Disponível em: <https://youtu.be/53IwjqFAYoQ>. Obviamente que tal apresentação, assim como a vigente subseção do presente artigo, não intenciona esgotar o tema.

utilizadas no tempo presente. As definições foram consideradas explícitas quando um artigo apresentava uma concepção de guerra cibernética distinta, declarada e inequívoca. Já a categoria de definição implícita foi usada para agrupar as concepções de guerra cibernética apresentadas nos artigos em que uma definição explícita não estava presente, o que significa que as definições implícitas podem ser inferidas a partir dos próprios textos (HUGHES; COLARIK, 2017).

A partir do levantamento dos significados existentes de guerra cibernética, Hughes e Colarik (2017) listaram e hierarquizaram as cinco definições de guerra cibernética mais influentes, pelo número de vezes que foram referenciadas:

Tabela 01 - As mais citadas definições de guerra cibernética

	Referência	**Definição**
1	Clarke e Knake (2010)	Ações de um Estado-Nação para penetrar nos computadores ou redes de outra nação com o objetivo de causar danos ou interrupções.
2	Arquilla e Ronfeldt (1993)	A guerra cibernética refere-se à condução e preparação para conduzir operações militares de acordo com os princípios relacionados à informação.
3	Rid (2012)	Um ato de força potencialmente letal, instrumental e político conduzido por meio de código malicioso.
4	*US Department of Defense* [Departamento de Defesa dos EUA] (2010)	Operações de Rede de Computadores (ORC), incluindo Ataque de Rede de Computadores (ARC), Defesa de Rede de Computadores (DRC) e Exploração de Rede de Computadores (ERC).
5	Nye (2011)	Ações hostis no ciberespaço que têm efeitos que amplificam ou são equivalentes a uma grande violência cinética.

Fonte: elaboração própria com base em HUGHES; COLARIK, 2017.

O presente artigo destacará a primeira delas, isto é, a definição de guerra cibernética considerada a mais essencial e influente (entretanto, conforme apontado anteriormente, não necessariamente consensual, e também não significando que seja a melhor), pela quantidade de vezes que foi citada: 830 citações (HUGHES; COLARIK, 2017), possivelmente sendo este número maior, já que o trabalho de referência foi publicado cinco anos atrás: “Ações de um

Estado-Nação para penetrar nos computadores ou redes de outra nação com o objetivo de causar danos ou interrupções" (CLARKE; KNAKE, 2010, p. 8)[3].

Um questionamento que pode ser feito à definição de Clarke e Knake (2010) é que ela talvez não leve em conta a guerra como entendida por Carl von Clausewitz (1780-1831), consagrado pensador ocidental do fenômeno do conflito armado, autor do livro *Da Guerra* (1832), obra que pode ser sintetizada através do preceito "a guerra é uma simples continuação da política por outros meios" (CLAUSEWITZ, 1996, p. 27). Tal publicação tem valor pioneiro e fundador como alicerce de toda a reflexão estratégica do Ocidente, tornando "sua leitura absolutamente indispensável para o entendimento da guerra" (PROENÇA JR.; DINIZ; RAZA, 1999, p. 13). O livro de Clarke e Knake, "*Cyberwar: The Next Threat to National Security and What to Do About It*", foi publicado originalmente em 2010[4]. Nesta obra, o sobrenome Clausewitz é mencionado apenas uma única vez, no início do capítulo cinco (intitulado "Em Busca de Uma Estratégia de Defesa"):

> Militares teóricos e estadistas, de Sun Tzu a von Clausewitz e Herman Kahn, durante séculos definiram e redefiniram várias formas de estratégias militares, mas todos tendem a concordar que elas envolvem uma ligação entre objetivos, meios (amplamente definidos), (talvez) limites e possivelmente um sequenciamento. Em suma, a estratégia militar é uma teoria integrada sobre o que queremos fazer e, em geral, como planejamos fazer isso (CLARKE; KNAKE, 2010, p. 72).

Conforme Thomas Rid (2012), o mundo nunca teria vivenciado um ato de guerra cibernética, o qual precisaria ser violento, instrumental e politicamente atribuído, consoante a visão clausewitziana. De acordo com esta linha de raciocínio, ofensivas cibernéticas seriam apenas variantes mais aprimoradas de três atividades tão longevas quanto a própria guerra: sabotagem, espionagem e subversão[5].

[3]Essa é a definição resumida. A definição mais ampla, dos mesmos autores, é: "Guerra cibernética é a penetração não autorizada – por, em nome de ou em apoio a um governo – de um computador, ou uma rede de computadores, de outra nação, ou qualquer outra atividade que afete um sistema de computador – atividade esta na qual o objetivo é adicionar, alterar ou falsificar dados, ou causar alguma ruptura ou dano a um computador, a algum dispositivo de rede ou aos objetos controlados por um sistema de computadores".

[4]Há uma edição brasileira, "Guerra Cibernética: A Próxima Ameaça à Segurança e o Que Fazer a Respeito", publicada em 2015.

[5]Uma visão semelhante e mais recente foi desenvolvida por Maschmeyer (2022), para quem "a característica distintiva da subversão é sua confiança na exploração secreta de vulnerabilidades em sistemas adversários" (não paginado). Ainda segundo tal estudioso, "A subversão pode produzir uma ampla gama de efeitos: pode influenciar a política e a opinião pública, sabotar a infraestrutura, perturbar a economia e fomentar distúrbios – pode até derrubar governos. Como resultado, a subversão é uma opção quase irresistível: é mais barata e de menor risco do que a guerra, mas ainda capaz de enfraquecer significativamente os adversários" (não paginado).

Primeiro: a sabotagem é um esforço que visa a enfraquecer ou destruir um sistema econômico ou militar. Segundo: a espionagem é uma ação que busca penetrar um sistema adversário com o objetivo de extrair informações sensíveis ou protegidas. Terceiro: a subversão é a tentativa determinada a abalar a autoridade, integridade e a constituição de uma autoridade ou ordem estabelecida, podendo a meta final ser a derrubada de um governo estabelecido (RID, 2012).

Todavia, a caracterização de guerra cibernética feita por Clarke e Knake (2010) pode evitar a problematização apontada previamente se for entendida no contexto da guerra híbrida[6] – fenômeno compreendido, essencialmente, como a dissolução das fronteiras entre política, guerra e paz. A guerra híbrida envolve técnicas de guerra regular e irregular, abrangendo o uso de operações psicológicas, como a infiltração na percepção do inimigo, para moldá-lo e paralisá-lo com bombas cognitivas de natureza informacional. Também engloba a chamada abordagem indireta[7], incluindo o uso de agentes terceirizados (como grupos de hackers recrutados pelos Estados, por exemplo) e não militares, de modo a promover ações de guerra não convencional em seus respectivos campos, como o direito, economia e comunicações (LEIRNER, 2020). O ciberespaço não é formado por um binário entre guerra e paz, mas sim por um espectro entre essas duas extremidades, sendo que a maioria das ofensivas digitais ocorre em algum lugar nesse espaço "cinzento" (GORDON; ROSENBACH, 2022).

Resumindo, por um lado, se for levada em consideração a definição de Clarke e Knake (2010) no contexto de guerra híbrida, é possível se referir às operações digitais ofensivas como guerra cibernética propriamente dita[8] (ou "guerra híbrida cibernética"[9]). Por outro lado, se for levada em consideração a problematização de Rid (2012) no contexto da guerra como entendida por Clausewitz, então as operações ofensivas no ciberespaço devem ser interpretadas como sabotagem, espionagem ou subversão. Este artigo considera que ambos os recortes são válidos e juntos permitem uma compreensão mais ampla do fenômeno.

[6]Essa expressão não chega a ser mencionada no livro *Cyberwar* (2010).
[7]Lembrar de B. H. Liddel Hart e seu livro *Strategy: The Indirect Approach*, publicado originalmente em 1929.
[8]Nos últimos anos, aproximadamente a partir de 2010, a ampliação no uso de telefones celulares e *smartphones* (e seus meios de informação) pelos indivíduos ao redor do mundo significou a extensão crucial das percepções dessas pessoas. Dessa forma, não há mais como pensar em uma guerra sem englobar o contexto informacional e eletrônico embutido nessa "extensão dos sentidos por outros meios" (comentário do professor Piero Leirner ao ler uma versão preliminar deste artigo). Não à toa, o embate armado entre a Rússia e a Ucrânia foi inicialmente chamado de guerra "TikTok", já que muitos portadores de telefones móveis acompanhavam o conflito através de vídeos postados em tal aplicativo.
[9]Rohozinski (2022), examinando a guerra entre a Rússia e a Ucrânia, também usou essa designação.

Além das percepções mostradas anteriormente, no contexto do levantamento de significados de guerra cibernética feito pelo autor deste artigo (ver nota de rodapé no. 2), outras definições interessantes encontradas foram as seguintes:

> A guerra cibernética é uma extensão da política através de ações tomadas no ciberespaço por atores estatais (ou atores não estatais com orientação ou apoio estatal significativo) que constituem uma séria ameaça à segurança de outro Estado, ou uma ação da mesma natureza tomada em resposta a uma séria ameaça à segurança de um Estado (real ou percebida) (GREEN, 2015, p. 2).
> Guerra cibernética é iniciada por um ator político usando meios cibernéticos com uma intenção coercitiva através da interrupção, manipulação, degradação ou destruição de informações, sistemas e processos baseados em informações ou objetos controlados ciberneticamente para atingir objetivos táticos, operacionais ou estratégicos contra um ator político para alcançar um fim político (HUGHES, 2017, p. 80).

Interessante notar que o conflito armado entre a Rússia e a Ucrânia trouxe novamente à tona o debate sobre como definir guerra cibernética (SMALLEY, 2022).

3 A guerra cibernética entre a Rússia e a Ucrânia em 2022

3.1 Primeira hipótese: não aconteceu como se esperava

O confronto bélico russo-ucraniano no campo digital não se desenvolveu como diversos analistas ocidentais imaginavam (THE ECONOMIST, 2022; ZAPPONE, 2022), isto é, sob a forma de uma espécie de "armagedom cibernético" (RM STAFF, 2022; ROHOZINSKI, 2022). Conforme apontou Jeremy Fleming, chefe da agência britânica de inteligência de sinais GCHQ (*Government Communications Headquarters* – Sede de Comunicações do Governo), a capacidade de Moscou em desencadear ataques cibernéticos devastadores à infraestrutura militar e civil da Ucrânia pode ter sido exagerada (embora fique a dúvida se essa avaliação é verdadeira ou se é parte de uma campanha de desinformação ocidental para depreciar a Rússia), talvez até mesmo o conceito de uma guerra cibernética tenha sido desmedido (SRIVASTAVA, 2022).

Provavelmente a Rússia realizou ataques cibernéticos menos rígidos e em menor quantidade do que poderia. Ainda não é devidamente conhecida a extensão do que aconteceu no campo de batalha cibernético neste conflito. É improvável que tudo o que os russos possam estar fazendo tenha se tornado público. Os detalhes factuais da dimensão cibernética da guerra podem eventualmente ser divulgados até ou após o fim do conflito (MALLICK, 2022).

De qualquer forma, antes e depois da invasão militar russa da Ucrânia, a Internet e outras infraestruturas críticas essenciais do Estado atacado prosseguiram operando, o comando e

controle das Forças Armadas ucranianas não descontinuou suas atividades e a desinformação da Rússia não persuadiu a população do país invadido de que a resistência seria improdutiva (MENN; TIMBERG, 2022). Afinal, o que explica isso? Foram identificadas basicamente nove razões (podendo haver outras, obviamente), que serão mostradas a seguir, pelas quais a violência no campo de batalha físico talvez não tenha sido apoiada na mesma medida por uma ofensiva *online*.

(i) O Kremlin se percebia como o "libertador": Moscou pode ter adotado uma postura modesta no espaço cibernético por razões estratégicas ou porque a linha do tempo para a invasão foi tão fugaz que as equipes de operações cibernéticas russas não sabiam o que atacar ou quando. No geral, acredita-se que Forças Armadas invasoras possam cortar rapidamente os cabos de *backbone* ("espinha dorsal" – trata-se do esquema de ligações centrais de um sistema mais amplo de redes de computadores) ou os desligue por meio de *hacking*, mas nada disso veio a acontecer na Ucrânia (MENN; TIMBERG, 2022). Considerando que o Kremlin se percebia como o libertador ucraniano, talvez nada disso fosse inevitável.

(ii) A Ucrânia estava preparada para se defender: Houve algumas ofensivas cibernéticas. A empresa de comunicação por satélite Viasat foi atacada no início da guerra. No dia 12 de abril de 2022, a Equipe de Resposta a Emergências de Computadores da Ucrânia frustrou um ataque cibernético do grupo russo *Sandworm* (um agremiado *hacker* que opera como *proxy* de Moscou) que visava "apagar" o país (desligar o fornecimento de eletricidade). A defesa cibernética ucraniana talvez tenha obtido um resultado melhor do que o esperado porque Kiev se concentrou em aperfeiçoar sua proteção no ciberespaço depois que *hackers* russos interromperam rapidamente a energia em regiões ucranianas nos anos de 2015 e 2016 (MENN; TIMBERG, 2022). Certamente a Rússia trava com a Ucrânia uma espécie de guerra cibernética há muito tempo. Segundo afirmou John Hultquis, da empresa de segurança cibernética *Mandiant*, "está cada vez mais claro que uma das razões pelas quais os ataques na Ucrânia foram moderados é porque os defensores de lá são muito agressivos e muito bons em confrontar os atores russos" (VOLZ; MCMILLAN, 2022, não paginado). A maioria das análises subestimou tanto os efeitos do aprendizado da Ucrânia, já que foi alvo da experimentação cibernética russa por anos[10], quanto o papel das medidas defensivas (ROHOZINSKI, 2022).

[10]Em 2017, o que inicialmente se achou que era um *ransomware* (*software* malicioso que bloqueia os dados de um alvo até que um resgate seja pago, geralmente em criptomoedas), mas que depois se revelou ser um *wiper* (*malware* que não possibilita a reversão do travamento dos dados), chamado *NotPetya*, cujo emprego foi atribuído à inteligência militar russa (GRU) para atacar a Ucrânia (NAKASHIMA, 2018), fugiu ao controle, acabando por se disseminar pelo mundo afora. Infectou uma gama diversificada de companhias multinacionais, incluindo a empresa de transporte global Maersk, a gigante farmacêutica Merck, a subsidiária europeia da FedEx, TNT Express, entre outras. Estima-se que tenha gerado mais de US$ 10 bilhões de prejuízos globalmente, sendo

(iii) Os ucranianos receberam apoio: a colaboração da Ucrânia com equipes cibernéticas defensivas do exterior é um potencial divisor de águas que pode ter impedido o sucesso de operações cibernéticas hostis de Moscou. Este é um ponto que vale a pena ser aprofundado em estudos futuros (MASCHMEYER; CAVELTY, 2022). Embora a cooperação ucraniana com outros países na área cibernética seja anterior à invasão militar russa, vale notar que, no início de março de 2022, anunciou-se que a Ucrânia foi aceita como participante contribuinte do Centro de Excelência em Defesa Cibernética Cooperativa (CCDCOE) da Organização do Tratado do Atlântico Norte (OTAN) (CISO ADVISOR, 2022). Aliás, cabe destacar que, em entrevista à *Sky News*, o chefe do Comando Cibernético dos Estados Unidos (*USCYBERCOM*), general Paul Nakasone, que também dirige a *National Security Agency* (NSA), órgão de inteligência de sinais dos EUA, admitiu pela primeira vez que militares norte-americanos conduziram uma série de operações (ofensivas, defensivas e de informações) no ciberespaço para apoiar a Ucrânia em seu esforço de guerra contra Moscou (MARTIN, 2022).

(iv) A Rússia poderia não querer destruir os serviços que planejava explorar: Moscou pode ter achado que os ucranianos cederiam tão rapidamente que não seria necessário danificar as infraestruturas que os russos gostariam de operar assim que uma ocupação começasse (obviamente se ocupar o país fosse o objetivo do Kremlin), já que sistemas de telecomunicações desativados e/ou bombardeados podem exigir reparos dispendiosos e lentos, bem como a imposição de sanções à Rússia dificultaria ainda mais tais consertos. Além disso, Moscou poderia demandar um sistema de telecomunicações operacional, abrangendo *links* de dados de alta velocidade, para uso próprio. Deste ângulo, imagens difundidas nas redes sociais e na imprensa chegaram a mostrar soldados russos em território ucraniano ao que tudo indica usando *smartphones*. As forças armadas contemporâneas possuem sistemas de rádios sofisticados para comunicabilidade no campo de batalha, mas lapsos das forças invasoras podem ter obrigado os russos a usarem sistemas alicerçados na Internet (MENN; TIMBERG, 2022).

(v) Uma ampla ofensiva cibernética afetaria a coleta de inteligência: até mesmo o uso de armas cibernéticas mais avançadas pode apresentar inconveniências, isto é, um sistema desativado por um pirata de computador não pode ser usado para coleta ininterrupta de inteligência, atividade normalmente prioritária em tempos de guerra (MENN; TIMBERG, 2022).

considerado o ataque cibernético mais devastador da história (GREENBERG, 2018), não porque tenha causado mortes ou destruição física, mas pelos danos econômicos.

(vi) Moscou deixou os ataques cibernéticos em "modo de espera": o Kremlin eventualmente preservou suas armas cibernéticas mais sofisticadas para uso contra as potências ocidentais, especialmente os EUA, em um ocasional estágio posterior da guerra, caso esta viesse a escalar, eventualmente podendo envolver a OTAN (ZAPPONE, 2022).

(vii) Em uma guerra brutal, a dimensão cibernética pode não ser necessária: a experiência cibernética da Rússia permitiu uma considerável vantagem quando Moscou *hackeou* nações rivais em tempos de paz. Entretanto, em uma situação de guerra, com o uso de violência real na Ucrânia, os ataques cibernéticos talvez sejam desnecessários. A atual estratégia da Rússia de reduzir as cidades ucranianas a escombros não requer um componente *online* (ZAPPONE, 2022).

(viii) As tropas cibernéticas russas foram superestimadas: a razão para a falta de uma agressão cibernética mais intensa da parte russa se deveu a um planejamento no nível cibernético que não foi tão bom quanto o esperado. Da mesma forma que os militares da Rússia surpreenderam o mundo com uma estratégia militar que aparentemente revelou inúmeros lapsos, talvez da mesma forma as tropas cibernéticas de Putin não estejam à altura de sua reputação (ZAPPONE, 2022).

(ix) A epidemia de *ransomware* alertou o mundo: os ataques de *ransomware* ajudaram a tornar a segurança cibernética uma prioridade política. Gangues de *ransomware* operam enganando organizações para fazer o download de *software* que bloqueia os dados confidenciais das vítimas. O programa malicioso é desbloqueado apenas se um resgate for pago. Esses criminosos cibernéticos, muitos ligados a Estados, ficaram cada vez mais sofisticados nos últimos anos. Depois que Joe Biden assumiu a presidência dos EUA no início de 2021, ele alçou o *ransomware* ao topo da agenda do G7[11], bem como em sua cúpula com Vladimir Putin (ZAPPONE, 2022).

3.2 Segunda hipótese: o mito da guerra cibernética ausente

A surpresa inicial de que a Rússia não lançou um ataque cibernético total para paralisar a infraestrutura ucraniana quando a guerra começou foi substituída por um entendimento de que houve uma atividade digital muito mais agressiva do que se pensava. Não foi um ataque maciço, contudo tem havido um conflito sustentado (CORERA, 2022). A Rússia pode estar

[11]O Grupo dos Sete é o conjunto dos países mais industrializados do mundo, formado por: Alemanha, Canadá, Estados Unidos, França, Itália, Japão e Reino Unido, sendo que a União Europeia também está representada.

conduzindo um longo jogo na frente cibernética, com ataques em andamento, mas ainda não totalmente compreendidos (PAUL, 2022).

Esta linha de raciocínio foi desenvolvida particularmente por David Cattler e Daniel Black no artigo "*The Myth of the Missing Cyberwar*" ("O Mito da Ciberguerra Desaparecida", em tradução livre), publicado na revista *Foreign Affairs* em 06 de abril de 2022. O referido texto inspirou o subtítulo logo acima e será a base desta seção do presente escrito. Uma visão semelhante foi desenvolvida por Rid (2022), o qual aponta que a guerra cibernética russo-ucraniana está acontecendo, mas nas sombras, por isso que não se fala tanto dela.

Muitas das evidências disponíveis apontam que a Rússia empregou uma campanha cibernética coordenada destinada a proporcionar às suas forças uma vantagem inicial durante a guerra na Ucrânia. A magnitude das operações *online* destrutivas pré-cinéticas[12] de Moscou foi sem precedentes (CATTLER; BLACK, 2022).

Os efeitos cumulativos desses ataques chamaram a atenção. Nas horas anteriores à invasão, a Rússia atingiu uma série de alvos importantes na Ucrânia, tornando inoperantes os sistemas de computadores de vários setores governamentais, militares e de infraestrutura crítica. Por exemplo, a sabotagem cibernética derrubou o provedor de Internet via satélite KA-SAT (da empresa norte-americana Viasat), do qual as unidades militares, de inteligência e policiais ucranianas dependem. Essa ofensiva também paralisou inúmeros *modems* de internet via satélite na Ucrânia e em toda a Europa (PEARSON; BING, 2022)[13].

Se os observadores veem a ciberofensiva russa na Ucrânia como uma série de eventos isolados, sua escala e significado estratégico se perdem na violência convencional que se desenrola no teatro de operações. Mas uma contabilidade integral das operações cibernéticas revela o uso proativo e persistente de ataques digitais para apoiar os objetivos militares russos (CATTLER; BLACK, 2022).

A percepção errônea de que a Rússia foi contida ou ineficaz no processo de sua guerra cibernética na Ucrânia provavelmente decorre do fato de que as operações digitais russas não

[12]O direcionamento cinético refere-se à aplicação direcionada de força militar com base na liberação ou concentração de energia cinética contra forças ou objetos opostos com efeitos (principalmente) letais no domínio físico.

[13]O empresário Elon Musk disponibilizou à Ucrânia o serviço de internet baseado em satélites *Starlink*, com a operação de aproximadamente 10.000 terminais em solo ucraniano. Ao contrário das torres de transmissão de telefonia celular, as antenas parabólicas usadas pelas forças ucranianas para a recepção do sinal vindo do espaço cósmico são pequenas e facilmente móveis para evitar detecção e retaliação. Isso manteve os hospitais danificados conectados e serviu como um *link* para veículos aéreos não tripulados desferirem ataques de artilharia contra os russos. A força de reconhecimento aéreo da Ucrânia usou o *Starlink* para se conectar diretamente a *drones* que arrasaram diversos tanques russos, centros de comando móveis e outros veículos militares (WADHWA; SALKEVER, 2022).

geraram os efeitos autônomos e debilitantes que as avaliações antes do conflito armado imaginavam que haveria. Mas essas considerações representam uma análise não realista do verdadeiro potencial estratégico das ofensivas *online* (CATTLER; BLACK, 2022).

Os erros da Rússia quase certamente prejudicaram sua capacidade em usar plenamente seu programa cibernético em apoio às suas forças convencionais. Porém, mesmo com essas limitações, as unidades russas de operações cibernéticas atacaram com sucesso uma série de alvos de acordo com os planos de guerra de Moscou. Os ataques cibernéticos russos a centros ucranianos de comando e controle governamentais e militares, logística, unidades de emergência e outros serviços críticos, como estações de controle de fronteira, foram consistentes com a chamada estratégia de "corrida de trovão"[14], destinada a alimentar o caos, a confusão, a incerteza e, em última análise, evitar uma guerra cara e prolongada na Ucrânia (CATTLER; BLACK, 2022) – embora seja isso que se observa atualmente.

Os ataques cibernéticos da Rússia antes da invasão sugerem preparações metódicas, com os atacantes provavelmente obtendo acesso às redes ucranianas com meses de antecedência. Por exemplo, unidades cibernéticas russas não chegaram a desligar a eletricidade ou a conectividade com a Internet em grande escala na Ucrânia. Entretanto, isso não significa que a Rússia seja incapaz de tais medidas, como alguns observadores sugeriram, mas que vislumbrou uma vitória rápida (o que acabou não acontecendo) e não viu a necessidade de interrupções tão amplas e indiscriminadas (CATTLER; BLACK, 2022)[15].

Enfim, de acordo com a perspectiva do "mito da guerra cibernética ausente", as operações digitais foram o maior sucesso militar da Rússia até os dias de hoje na guerra na Ucrânia (CATTLER; BLACK, 2022).

3.3 Terceira hipótese: síntese das anteriores

Com base no que foi exposto previamente e no que será apontado a seguir, este artigo lança uma terceira hipótese de trabalho: o que está havendo como extensão do conflito armado

[14]De acordo com o dicionário urbano, essa expressão significa "Um comboio militar de alta velocidade utilizando armas pesadas, veículos blindados e táticas ofensivas para chegar a um destino, provavelmente ao longo de uma rota de extremo perigo. A força, velocidade e intensidade do ataque, juntamente com o uso de armas e equipamentos formidáveis, rapidamente superam a aturdida força defensiva". Tal definição pode ser encontrada em: <https://www.urbandictionary.com/define.php?term=Thunder%20Run>.

[15]Ao examinar versão preliminar deste artigo, o Professor Piero Leirner (UFSCar) fez uma ponderação importante: como não se conhece exatamente o que os russos estão buscando, fica difícil avaliar se a manutenção dessa infraestrutura não foi pensada justamente num quadro mais geral de "operação psicológica", que justamente não visava um "choque e pavor".

russo-ucraniano é uma forma de guerra cibernética mais "branda", ou de baixa intensidade[16], que pode ser entendida tanto no sentido do entendimento de Clarke e Knake (2010) no contexto de guerra híbrida (aí podendo ser designada de guerra cibernética, ou "guerra híbrida cibernética"[17]) quanto na acepção de sabotagem, espionagem e subversão conforme sugerida por Rid (2012) em sua linha clausewitziana (neste caso, acredita-se que a designação mais adequada não seria guerra cibernética, mas sim operações cibernéticas ofensivas), bem como nas definições de Green (2015) e Hughes (2017).

A hipótese da guerra cibernética mais "branda" é uma espécie de síntese entre as hipóteses apontadas nas duas subseções anteriores. Trata-se de um conflito de baixa intensidade no sentido do que poderia ter sido, mas não foi (conforme apontado em 3.1), não significando que não esteja acontecendo ou que não tenha um considerável nível de expressividade (de acordo com o mostrado em 3.2).

Desde que a guerra russo-ucraniana começou, o "pior" não aconteceu. Moscou não "derrubou" a rede elétrica ucraniana e não causou uma "catástrofe" cibernética global como o *NotPetya* em 2017 (VOLZ; MCMILLAN, 2022). A maioria dos ataques russos se concentrou em perturbações, espionagem e desinformação. Seu efeito tem sido principalmente cognitivo e psicológico (o que não deixa de ser significativo, pois na guerra híbrida o centro de gravidade costuma ser a opinião pública ou o ambiente informacional), e ao que tudo leva a crer não terá condições de decidir a guerra. Aparentemente não há indicação de que qualquer uma dessas ofensivas tenha ajudado a Rússia estrategicamente no campo de batalha físico (ABBANY, 2022), embora tenham impactado o ecossistema de informações.

Foram identificadas basicamente três categorias principais de táticas cibernéticas utilizadas até agora: limpadores (*wipers*), ataques DDoS (sigla em inglês para *distributed denial of service* – negação de serviço distribuída) e desfiguração (*defacement*), sendo que cada delas uma será explicada a seguir.

Os limpadores (*wipers*) objetivam excluir informações em uma rede de computadores, impossibilitando que os usuários possam acessar seus próprios dados. A estratégia de limpeza inclui o uso de *ransomwares*, isto é, *malwares* (*malicious softwares* – programas maliciosos) que bloqueiam os dados de um alvo até que um resgate seja pago, geralmente em criptomoedas. A utilização de limpadores sugere que o Kremlin vinha preparando algumas de suas investidas cibernéticas há meses. Isso pressupõe que tais ofensivas estão consistentemente arraigadas na

[16]Apesar da "baixa intensidade", a guerra russo-ucraniana teve efeitos notáveis no cenário global de ameaças cibernéticas, apontou o Relatório de Ameaças do primeiro trimestre de 2022 da Avast (CISO ADVISOR, 2022 b).
[17]Rohozinski (2022), avaliando a guerra russo-ucraniana, também usou essa expressão.

estratégia de guerra de Moscou. Os ataques do tipo *ransomware* implicam – mas não necessariamente confirmam – um elemento criminoso na guerra (por exemplo, o uso de grupos hackers que atuam como *proxies* de Moscou), que pode ou não estar associado ao governo russo (a atribuição é uma das partes mais desafiadoras em uma guerra cibernética) (ABBANY, 2022)[18].

Os ataques DDoS (*distributed denial of service* – negação de serviço distribuída) são usados para deixar sites fora do ar. Essa forma de ofensiva cibernética envolve sobrecarregar um sistema através de um elevado número de "solicitações" – *botnets*[19] buscando acessar um domínio na Internet – em um reduzido período de tempo. Se esse cômputo de acessos exceder o limite que o sistema pode aguentar, ele para de responder. Logo, para o mundo externo, o sistema acaba desligando. Trata-se de um método de ataque cibernético habitual e descomplicado (ABBANY, 2022).

Os ataques de desfiguração (*defacement*) eliminam ou modificam as informações em um site. É uma ferramenta básica de desinformação que tem a capacidade de levar os internautas a acreditarem que dados incorretos são verdadeiros. E isso pode se espalhar de forma rápida. Trata-se de uma técnica antiga usada nos confrontos armados, sendo chamada de "ofuscação", quando os lados de um conflito bélico abarrotam uma determinada população civil com informações enganosas. O efeito é basicamente psicológico e muito eficaz (ABBANY, 2022).

O trabalho "*Goodbye Cyberwar: Ukraine as Reality Check*" ("Adeus ciberguerra: Ucrânia como verificação da realidade", em tradução livre), de Lennart Maschmeyer e Myriam Dunn Cavelty (2022), apoia a terceira hipótese aqui apresentada.

Embora as operações cibernéticas permaneçam sendo importantes para ações de inteligência e ofensivas de baixa intensidade, ataques cibernéticos destrutivos direcionados a infraestruturas militares ou civis relevantes são difíceis de implementar e ineficazes quando comparados aos ataques convencionais, e talvez por isso que não se tenha observado esse tipo de ofensiva cibernética na guerra Rússia x Ucrânia em 2022. O motivo é um trilema[20] operacional (MASCHMEYER, 2021) que restringe a velocidade, intensidade e controle que as

[18]Aqui cabe destacar o *WhisperGate*: "O malware Wiper, apelidado de WhisperGate pela Microsoft, foi colocado nos sistemas ucranianos em 13 de janeiro de 2022. O limpador foi projetado para se parecer com um *ransomware* e ofereceu às vítimas o que parecia ser uma maneira de descriptografar seus dados através do pagamento de um valor, embora, na realidade, o *malware* tenha apagado o sistema. O limpador foi encontrado em sistemas em toda a Ucrânia, incluindo o Ministério das Relações Exteriores e redes usadas pelo gabinete ucraniano. Os dois limpadores usados no WhisperGate têm semelhanças com o limpador NotPetya que atingiu a Ucrânia e várias grandes empresas multinacionais em 2017" (FENDORF; MILLER, 2022, não paginado).

[19]Do inglês *robot networks*, significa "redes de robôs", quer dizer, uma rede de computadores privados infectados com *software* malicioso e controlados como um grupo sem o conhecimento dos proprietários.

[20]Situação problemática, em que é preciso escolher uma de três formas para solucioná-la.

ações cibernéticas podem alcançar – limitando assim seu valor estratégico e tornando os ataques catastróficos altamente improváveis (MASCHMEYER; CAVELTY, 2022).

As intervenções cibernéticas oferecem vantagens estratégicas únicas porque são conduzidas secretamente e exploram os sistemas de computador do adversário para usá-los contra o próprio oponente. Dessa forma, para Maschmeyer e Cavelty (2022), as ofensivas digitais são principalmente instrumentos de subversão, e não de guerra[21]. No entanto, a exploração envolve um conjunto particular de obstáculos que criam um trilema operacional entre velocidade, intensidade e controle dos efeitos. Os atores só podem aumentar a eficácia de uma dessas variáveis sob o custo de diminuir as outras (MASCHMEYER; CAVELTY, 2022).

No geral, não há evidências (talvez com exceção do ataque à Viasat) de que qualquer uma das operações patrocinadas pela Rússia ou demais ofensivas relacionadas a esta contenda armada (incluindo os vários "exércitos" hacktivistas que surgiram[22]) afetaram de forma mensurável os rumos do conflito, forneceram vantagens táticas observáveis (como sabotar equipamentos militares ou interromper as comunicações inimigas durante a batalha) ou produziram valor estratégico (MASCHMEYER; CAVELTY, 2022).

Apesar das proeminentes expectativas, há evidências crescentes das limitações práticas dos ataques cibernéticos, tanto em ambientes híbridos quanto em guerra propriamente dita. Esta conclusão se aplica particularmente à guerra cibernética na forma de ataques destrutivos orientados a alvos específicos. Em contraste, espera-se que as operações disruptivas de baixa intensidade continuem a atormentar as redes de computadores em geral, com destaque para o *ransomware*[23], a ciberespionagem e as operações de influência cibernética usadas para ampliar divisões nas sociedades (MASCHMEYER; CAVELTY, 2022).

4 Considerações finais

Um aspecto remanescente para atentar é o papel das empresas de mídias sociais e tecnologia na guerra – que são parte do aspecto informacional e do campo de batalha das

[21]Lembrar Thomas Rid (2012) e sua linha clausewitziana. Por outro lado, se for levada em consideração a definição de Clarke e Knake (2010) no contexto de guerra híbrida (LEIRNER, 2020), aí talvez essas ações possam ser consideradas de guerra cibernética (ou "guerra híbrida cibernética") propriamente dita.

[22]Hackers ativistas organizaram um "Exército de TI [Tecnologia da Informação]" voluntário para hackear o governo russo e sites comerciais da Rússia, da mesma forma que o coletivo *Anonymous* declarou guerra cibernética ao Kremlin.

[23]Conforme observado pelo jornalista Paulo Brito, ao comentar versão preliminar deste artigo, talvez mais adequado do que indicar os *ransomwares*, seja fazer referência aos *wipers* (como o *NotPetya*). Alguns fingem, ou simulam, que são *ransomwares*. Entretanto, na verdade, são *wipers*, o que significa que não existe a chance de reversão da criptografia.

narrativas (CULLIFORD, 2022). O Facebook, por exemplo, restringiu o conteúdo proveniente da mídia estatal russa em todo o mundo (HAYS, 2022). Todavia não foi o único: Google, Microsoft, Netflix, TikTok, Twitter, Youtube, entre outras, também adotaram medidas semelhantes. Moscou, por sua vez, proibiu o acesso a partir de seu território ao Facebook e ao Twitter (G1, 2022).

Para além da guerra russo-ucraniana, mas igualmente levando-a em consideração, nota-se que as grandes empresas de tecnologia, como Alibaba, Amazon, Apple, Facebook, Google, Huawei, Instagram, TikTok, Twitter, etc passaram a exercer cada vez mais influência na esfera geopolítica (BREMMER, 2021), pois o que elas toleram ou desautorizam em seus "reinos" digitais podem influenciar os movimentos das relações internacionais (SINGER; BROOKING, 2018), embora o ator político mais importante continue sendo o Estado-Nação (WALT, 2021).

Concluindo, esta pesquisa buscou investigar a dimensão cibernética da guerra russo-ucraniana em 2022, especificamente os primeiros cem dias. A partir do levantamento bibliográfico e revisão da literatura (que ainda está surgindo, já que a guerra é recente e continua em andamento), foram mapeadas basicamente duas hipóteses sobre o assunto: a primeira afirma que a guerra cibernética não aconteceu como se esperava; a segunda aponta ser um mito a ausência de guerra cibernética. O autor deste trabalho buscou juntar elementos das hipóteses anteriores para lançar uma terceira hipótese de trabalho ("nem tanto ao mar, nem tanto à terra"), a qual pode ter alcance explicativo mais robusto do que as duas primeiras isoladamente: o que está se desenrolando como prolongamento do conflito bélico entre a Rússia e a Ucrânia é uma forma de guerra cibernética mais "branda", ou de baixa intensidade.

A fim de encerrar este artigo, vale registrar ponderação de Alperovitch (2022):

> Há uma verdade mais ampla sobre o papel das operações no ciberespaço nos conflitos militares modernos: não existe uma guerra cibernética pura. Há apenas guerra, travada com uma multiplicidade de ferramentas em variados domínios. A esse respeito, os ataques cibernéticos não são nem mesmo uma frente separada em um conflito convencional, mas sim uma extensão da própria guerra (não paginado).

* O autor agradece ao professor titular Piero de Camargo Leirner (UFSCar – Universidade Federal de São Carlos) e ao jornalista Paulo Brito (editor do portal *CISO Advisor*) pela leitura e comentários a versões preliminares do presente artigo, sendo a responsabilidade final inteiramente do criador deste trabalho. Também ficam registrados os agradecimentos à Roberta Carneiro de Melo (estudante de doutorado da UFF – Universidade Federal Fluminense) e ao Danilo Sorato (editor da revista *Hoplos*) pelo auxílio na solução de algumas dúvidas operacionais relativas à publicação do vigente texto.

Referências

ABBANY, Zulfikar. Ukraine: Cyberwar creates chaos, 'it won't win the war'. *Deutsche Welle*, 03 mar. 2022. Disponível em: <https://p.dw.com/p/47wg1>. Acesso em: 04 mar. 2022.

ALPEROVITCH, Dmitri. How Russia Has Turned Ukraine Into a Cyber-Battlefield. *Foreign Affairs*, 28 jan. 2022. Disponível em: <https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield>. Acesso em: 29 jan. 2022.

ARQUILLA, John; RONFELDT, David. Cyberwar is coming!. *Comparative Strategy*. Vol. 12, Issue 2, 1993, pp. 141-165. Disponível em: <https://doi.org/10.1080/01495939308402915>. Acesso em: 02 jun. 2022.

ASHRAF, Cameran. Defining cyberwar: towards a definitional framework. *Defense and Security Analysis*. Vol. 37, No. 3, 2021, pp. 274-294. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/14751798.2021.1959141>. Acesso em: 02 jan. 2022.

BREMMER, Ian. The Technopolar Moment: How Digital Powers Will Reshape the Global Order. *Foreign Affairs*. Vol. 100, Number 6, 2021. Disponível em: <https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order>. Acesso em: 02 jun. 2022.

CATTLER, David; BLACK, Daniel. The Myth of the Missing Cyberwar. *Foreign Affairs*, 06 abr. 2022. Disponível em: <https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar>. Acesso em: 07 abr. 2022.

CISO ADVISOR. Ucrânia entra para o centro de defesa cibernética da Otan. *CISO Advisor*, 08 mar. 2022. Disponível em: <https://www.cisoadvisor.com.br/ucrania-entra-para-o-centro-de-defesa-cibernetica-da-otan/>. Acesso em: 09 mar. 2022.

CISO ADVISOR. Guerra transforma cenário global de ameaças cibernéticas. *CISO Advisor*, 30 mai. 2022b. Disponível em: <https://www.cisoadvisor.com.br/guerra-transforma-cenario-global-de-ameacas-ciberneticas/>. Acesso em: 30 mai. 2022.

CLARKE, Richard; KNAKE, Robert. *Cyberwar: The Next Threat to National Security and What to Do About It*. New York: HarperCollins e-books, 2010.

CLAUSEWITZ, Carl von. *Da Guerra*. São Paulo: Martins Fontes, 1996.

CORERA, Gordon. Ukraine war: Don't underestimate Russia cyber-threat, warns US. *BBC News*, 11 mai. 2022. Disponível em: <https://www.bbc.com/news/technology-61416320>. Acesso em: 12 mai. 2022.

CULLIFORD, Elizabeth. Analysis: Moscow battles big tech to control the narrative. *Reuters*, 27 fev. 2022. Disponível em: <https://www.reuters.com/technology/russia-invades-ukraine-moscow-battles-big-tech-control-narrative-2022-02-28/>. Acesso em: 28 fev. 2022.

DONATO, Joseph M. Putin's Bad Math: the Root of Russian Miscalculation in Ukraine. *Modern War Institute at West Point*, 10 mai. 2022. Disponível em: <https://mwi.usma.edu/putins-bad-math-the-root-of-russian-miscalculation-in-ukraine/>. Acesso em: 10 mai. 2022.

FENDORF, Kyle; MILLER, Jessie. Tracking Cyber Operations and Actors in the Russia-Ukraine War. *Net Politics and Cyberspace Policy Program, Council on Foreign Relations (CFR)*, 24 mar. 2022. Disponível em: <https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war>. Acesso em: 25 mar. 2022.

FREEDMAN, Lawrence. Putin's war is in disarray. *The New Statesman*, 07 mar. 2022. Disponível em: <https://www.newstatesman.com/international-politics/geopolitics/2022/03/putins-war-is-in-disarray>. Acesso em: 8 mar. 2022.

G1. Rússia bloqueia acesso ao Facebook e ao Twitter. *G1*, 04 mar. 2022. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/03/04/facebook-e-bloqueado-na-russia-apos-agir-contra-midia-estatal-do-pais.ghtml>. Acesso em: 05 mar. 2022.

GORDON, Sue; ROSENBACH, Eric. America's Cyber-Reckoning. *Foreign Affairs*, Vol. 101, Number 1, 2022. Disponível em: <https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning>. Acesso em: 05 jan. 2022.

GREEN, James A. (Ed.). *Cyber Warfare: A multidisciplinary analysis*. London: Routledge, 2015.

GREENBERG, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, 22 ago. 2018. Disponível em: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>. Acesso em: 02 jun. 2022.

HALPERN, Sue. The Threat of Russian Cyberattacks Looms Large. *The New Yorker*, 22 mar. 2022. Disponível em: <https://www.newyorker.com/news/daily-comment/the-threat-of-russian-cyberattacks-looms-large>. Acesso em: 23 mar. 2022.

HAYS, Kali. Facebook demotes Russian state media across its platforms worldwide. *Business Insider*, 01 mar. 2022. Disponível em: <https://www.businessinsider.com/facebook-ukraine-russia-news-state-media-2022-3>. Acesso em: 02 mar. 2022.

HEDLUND, Stefan. The collapse of the Russian military machine. *Geopolitical Intelligence Services* (GIS), 02 mai. 2022. Disponível em: <https://www.gisreportsonline.com/r/russian-military-power/>. Acesso em: 03 mai. 2022.

HUGHES, Dan. A Discourse in Conflict: Resolving the Definitional Uncertainty of Cyber War. *Thesis, Master of Arts in Defense and Security Studies*. Massey University, Albany, 2017. Disponível em: <https://mro.massey.ac.nz/bitstream/handle/10179/12989/02_whole.pdf>. Acesso em: 02 jan. 2022.

HUGHES, Daniel; COLARIK, Andrew. The Hierarchy of Cyber War Definitions. In: WANG, G.; CHAU, M.; CHEN, H. (eds.). *Intelligence and Security Informatics. Lecture Notes in Computer Science*. Vol. 10241, 2017. Disponível em: <https://doi.org/10.1007/978-3-319-57463-9_2>. Acesso em: 02 jan. 2022.

JOHNSON, Daniel. Putin's catastrophic war has exposed Russia as a third-rate power. *The Telegraph*, 22 mai. 2022. Disponível em: <https://www.telegraph.co.uk/business/2022/05/22/putins-catastrophic-war-has-exposed-russia-third-rate-power/>. Acesso em: 23 mai. 2022.

JOHNSON, Rob. Dysfunctional Warfare: The Russian Invasion of Ukraine. *Parameters, The US Army War College Quarterly*. Vol. 52, No. 2, 2022. Disponível em: <https://press.armywarcollege.edu/parameters/vol52/iss2/8/>. Acesso em: 02 jun. 2022.

LEIRNER, Piero C. *O Brasil no Espectro de uma Guerra Híbrida: Militares, operações psicológicas e política em uma perspectiva etnográfica*. São Paulo: Alameda, 2020.

MALLICK, Maj Gen PK. Decoding Russia's 'Missing' Cyberwar Amid War in Ukraine. *VIF [Vivekananda International Foundation] Brief*, Maio de 2022. Disponível em: <https://www.vifindia.org/sites/default/files/Decoding-Russia-s-Missing-Cyberwar-Amid-War-in-Ukraine.pdf>. Acesso em: 02 jun. 2022.

MARKS, Joseph; SCHAFFER, Aaron. Some see cyberwar in Ukraine. Others see just thwarted attacks. *The Washington Post*, 14 abr. 2022. Disponível em: <https://www.washingtonpost.com/politics/2022/04/14/some-see-cyberwar-ukraine-others-see-just-thwarted-attacks/>. Acesso em: 15 abr. 2022.

MARTIN, Alexander. US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command. *Sky News*, 01 jun. 2022. Disponível em: <https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139>. Acesso em: 02 jun. 2022.

MASCHMEYER, Lennart; CAVELTY, Myriam Dunn. Goodbye Cyberwar: Ukraine as Reality Check. *Policy Perspectives*. *Center for Security Studies (CSS)*. Vol. 10/3, 2022, pp. 1-4. Disponível em: <https://css.ethz.ch/en/center/CSS-news/2022/06/goodbye-cyberwar-ukraine-as-reality-check.html>. Acesso em: 01 jun. 2022.

MASCHMEYER, Lennart. The Myth of Cyberwar and the Realities of Subversion. *Modern War Institute at West Point*. 24 jan. 2022. Disponível em: <https://mwi.usma.edu/the-myth-of-cyberwar-and-the-realities-of-subversion/>. Acesso em: 25 jan. 2022.

MASCHMEYER, Lennart. The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security*. Vol. 46, Issue 2, 2021, pp. 51-90. Disponível em: <https://direct.mit.edu/isec/article/46/2/51/107693/The-Subversive-Trilemma-Why-Cyber-Operations-Fall>. Acesso em: 02 nov. 2021.

MASUHR, Niklas; ZOGG, Benno. The War in Ukraine: First Lessons. *CSS Analyses in Security Policy*. No. 301, 06 abr. 2022. Disponível em: <https://css.ethz.ch/en/center/CSS-news/2022/04/the-war-in-ukraine-first-lessons.html>. Acesso em: 01 mai. 2022.

MENN, Joseph; TIMBERG, Craig. The dire predictions about a Russian cyber onslaught haven't come true in Ukraine. At least not yet. *The Washington Post*, 28 fev. 2022. Disponível em: <https://www.washingtonpost.com/technology/2022/02/28/internet-war-cyber-russia-ukraine/>. Acesso em: 01 mar. 2022.

NAKASHIMA, Ellen. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. *The Washington Post*, 12 jan. 2018. Disponível em: <https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html>. Acesso em: 01 jun. 2022.

NYE JR., Joseph S. Nuclear Lessons for Cyber Security?. *Strategic Studies Quarterly*. Vol. 05, Issue 4, 2011, pp. 18-38. Disponível em: <https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-4/Nye.pdf>. Acesso em: 01 jun. 2022.

PAUL, Kari. Russia's slow cyberwar in Ukraine begins to escalate, experts say. *The Guardian*, 02 abr. 2022. Disponível em: <https://www.theguardian.com/world/2022/apr/01/russia-ukraine-cyberwar>. Acesso em: 03 abr. 2022.

PEARSON, James; BING, Christopher. The cyber war between Ukraine and Russia: An overview. *Reuters*, 10 mai. 2022. Disponível em: <https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/>. Acesso em: 11 mai. 2022.

PROENÇA JR., Domício; DINIZ, Eugenio; RAZA, Salvador Ghelfi. *Guia de Estudos de Estratégia*. Rio de Janeiro: Jorge Zahar Ed., 1999.

RID, Thomas. Why You Haven't Heard About the Secret Cyberwar in Ukraine. *The New York Times*, 18 mar. 2022. Disponível em: <https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html>. Acesso em: 19 mar. 2022.

RID, Thomas. Cyber War Will Not Take Place. *Journal of Strategic Studies*. Vol. 35, Issue 1, 2012. Disponível em: <https://doi.org/10.1080/01402390.2011.608939>. Acesso em: 01 jun. 2022.

RM STAFF. Why Hasn't Russia Unleashed 'Cybergeddon' in Its War on Ukraine?. *Russia Matters*, *Harvard Kennedy School Belfer Center for Science and International Affairs*, 04 mai. 2022. Disponível em: <https://www.russiamatters.org/analysis/why-hasnt-russia-unleashed-cybergeddon-its-war-ukraine>. Acesso em: 10 mai. 2022.

ROBINSON, Michael; JONES, Kevin; JANICKE, Helge. Cyber warfare: Issues and challenges. *Computers and Security*. Volume 49, 2015, pp. 70-94. Disponível em: <https://www.tech.dmu.ac.uk/~rgs/ACECSR_publications/HelgeJanicke.pdf>. Acesso em: 02 jan. 2022.

ROHOZINSKI, Rafal. The missing ‘cybergeddon’: what Ukraine can tell us about the future of cyber war. *The Survival Editor’s Blog*; *International Institute for Strategic Studies (IISS)*, 09 mar. 2022. Disponível em: <https://www.iiss.org/blogs/survival-blog/2022/03/the-missing-cybergeddon-what-ukraine-can-tell-us-about-the-future-of-cyber-war>. Acesso em: 11 mar. 2022.

SHULTZ, Richard H.; BRIMELOW, Benjamin. Russia’s Potemkin Army. *Modern War Institute at West Point*, 23 mai. 2022. Disponível em: <https://mwi.usma.edu/russias-potemkin-army/>. Acesso em: 24 mai. 2022.

SINGER, P. W.; BROOKING, Emerson T. What Clausewitz Can Teach Us About War on Social Media. *Foreign Affairs*, 04 out. 2018. Disponível em: <https://www.foreignaffairs.com/articles/2018-10-04/what-clausewitz-can-teach-us-about-war-social-media>. Acesso em: 02 jan. 2022.

SMALLEY, Suzanne. Ukraine conflict spurs questions of how to define cyberwar. *CyberScoop*, 02 mar. 2022. Disponível em: <https://www.cyberscoop.com/russia-ukraine-cyberwar-nato-geneva-microsoft/>. Acesso em: 03 mar. 2022.

SRIVASTAVA, Mehul. Prospect of Russian cyber war may have been ‘overhyped’, says UK spy chief. *Financial Times*, 10 mai. 2022. Disponível em: <https://www.ft.com/content/d5657df5-a962-4acf-b0bd-b892c6b15361>. Acesso em: 11 mai. 2022.

THE ECONOMIST. Cyber-attacks on Ukraine are conspicuous by their absence. *The Economist*, 01 mar. 2022. Disponível em: <https://www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence>. Acesso em: 05 mar. 2022.

TZU, Sun. *A Arte da Guerra*. Porto Alegre: L&PM, 2006.

US DEPARTMENT OF DEFENSE. *Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms*. Washington: DoD, 2010. Disponível em: <https://irp.fas.org/doddir/dod/jp1_02.pdf>. Acesso em: 01 jun. 2022.

VOLZ, Dustin; MCMILLAN, Robert. In Ukraine, a ‘Full-Scale Cyberwar’ Emerges. *The Wall Street Journal*, 12 abr. 2022. Disponível em: <https://www.wsj.com/articles/in-ukraine-a-full-scale-cyberwar-emerges-11649780203>. Acesso em: 14 abr. 2022.

WADHWA, Vivek; SALKEVER, Alex. How Elon Musk's Starlink Got Battle-Tested in Ukraine. *Foreign Policy*, 04 mai. 2022. Disponível em: <https://foreignpolicy.com/2022/05/04/starlink-ukraine-elon-musk-satellite-internet-broadband-drones/>. Acesso em: 10 mai. 2022.

WALT, Stephen. Big Tech Won't Remake the Global Order. *Foreign Policy*, 08 nov. 2021. Disponível em: <https://foreignpolicy.com/2021/11/08/big-tech-wont-remake-the-global-order/>. Acesso em: 12 dez. 2021.

WOLFF, Josephine. Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine. *Time*, 02 mar. 2022. Disponível em: <https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/>. Acesso em: 05 mar. 2022.

ZAPPONE, Chris. Seven reasons Putin hasn't launched a cyberwar in Ukraine – yet. *The Sydney Morning Herald*, 25 abr. 2022. Disponível em: <https://www.smh.com.au/world/europe/seven-reasons-putin-hasn-t-launched-a-cyberwar-in-ukraine-yet-20220421-p5af3o.html>. Acesso em: 27 abr. 2022.

Recebido em 05 de junho de 2022.
Aceito para publicação em 13 de julho de 2022.